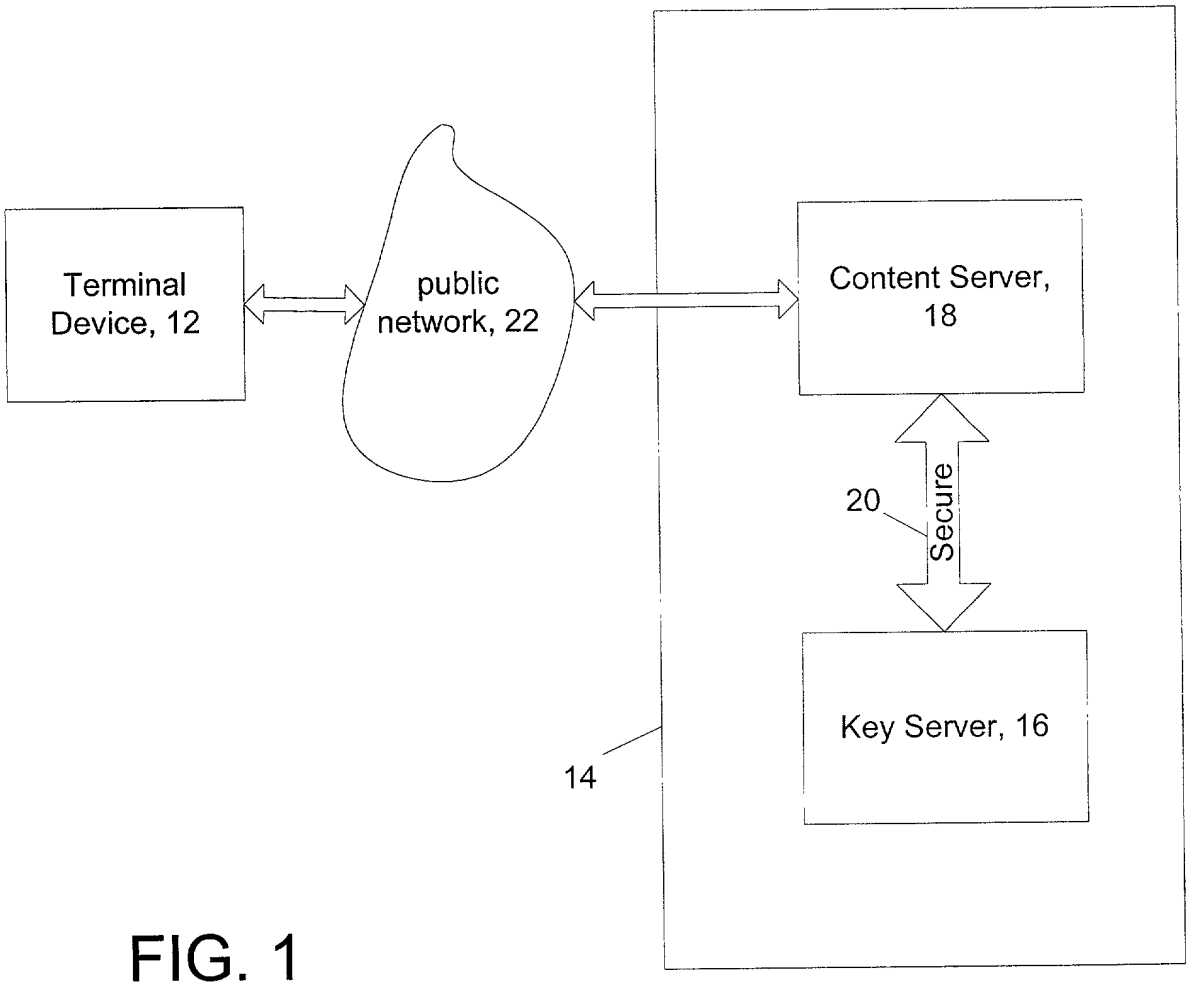

Terminal Device, 12
public network, 22
Content Server, 18
20
Secure
Key Server, 16
14

FIG. 1

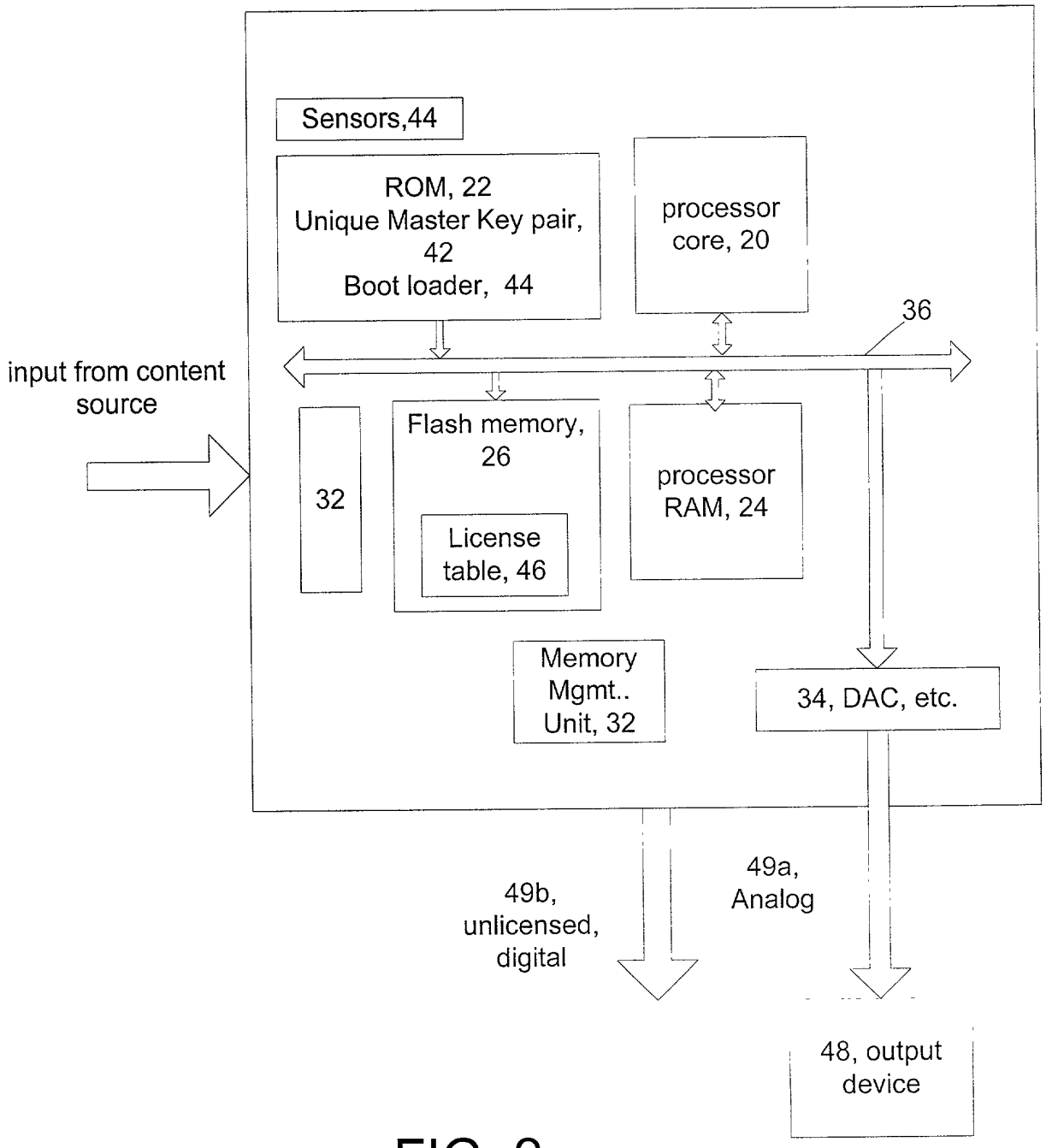

Sensors,44
ROM, 22
Unique Master Key pair, 42
Boot loader, 44
processor core, 20
36
input from content source
32
Flash memory, 26
License table, 46
processor RAM, 24
Memory Mgmt.. Unit, 32
34, DAC, etc.
49b, unlicensed, digital
49a, Analog
48, output device

FIG. 2

EXHIBIT 2008, Page 3 of 17

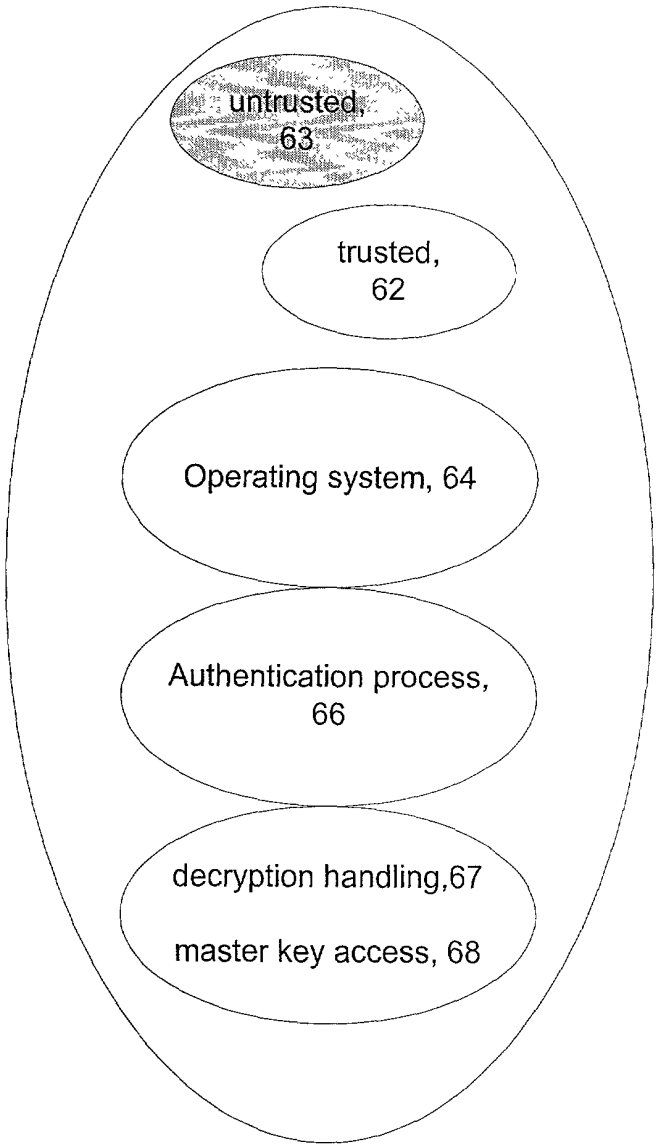


FIG. 3

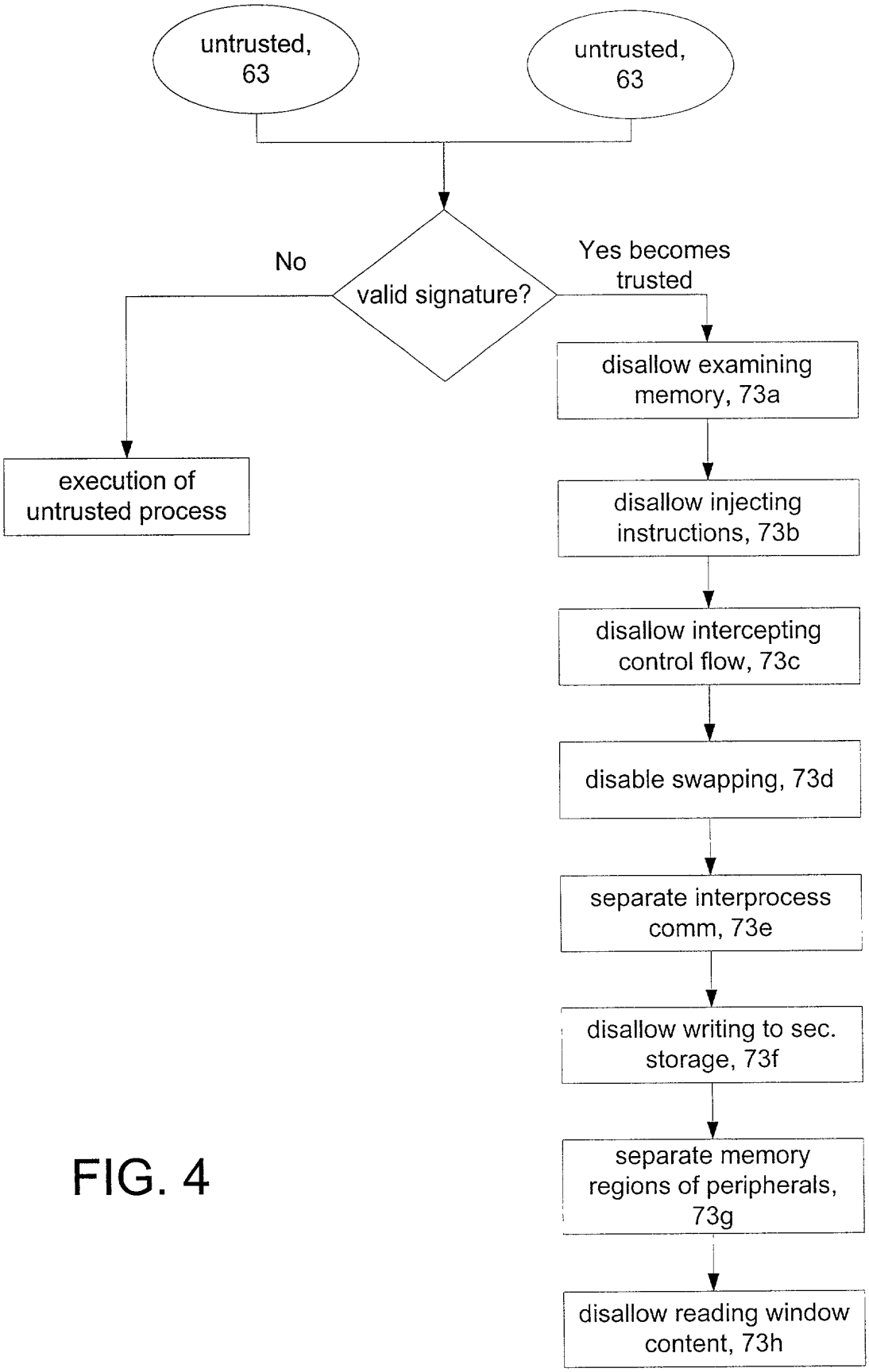

untrusted, 63
untrusted, 63
valid signature?
No
Yes becomes trusted
execution of untrusted process
disallow examining memory, 73a
disallow injecting instructions, 73b
disallow intercepting control flow, 73c
disable swapping, 73d
separate interprocess comm, 73e
disallow writing to sec. storage, 73f
separate memory regions of peripherals, 73g
disallow reading window content, 73h

FIG. 4

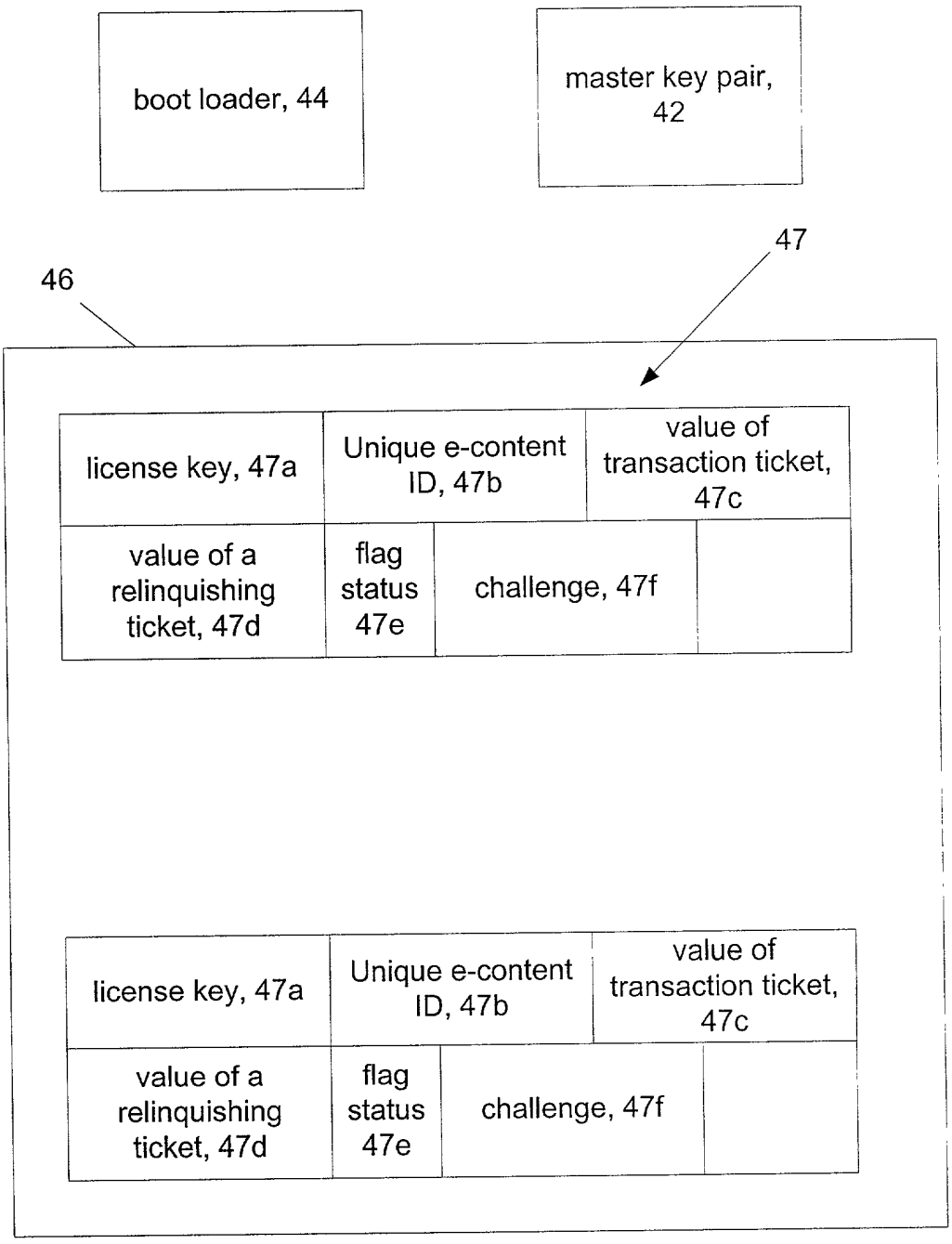
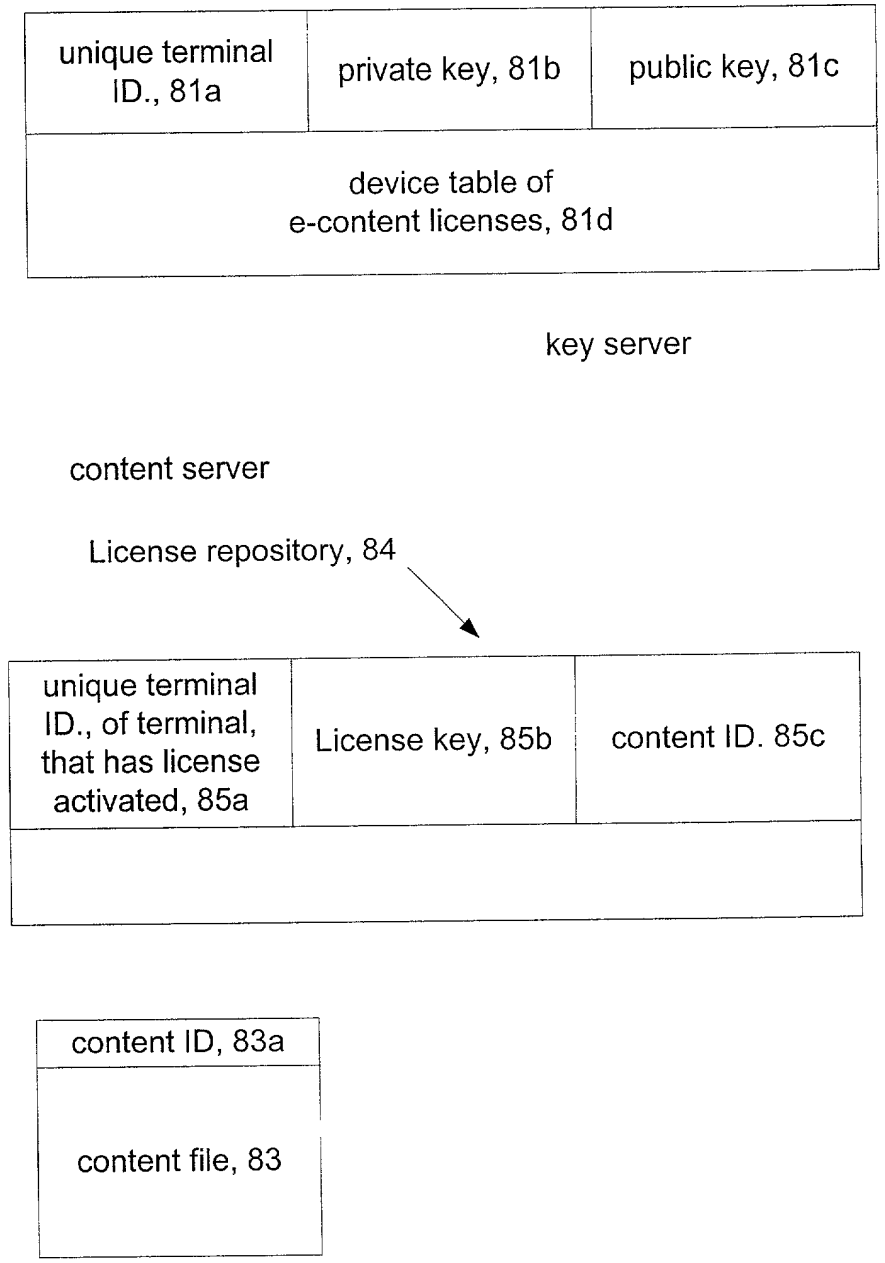

boot loader, 44
master key pair, 42
47
46
license key, 47a
Unique e-content ID, 47b
value of transaction ticket, 47c
value of a relinquishing ticket, 47d
flag status 47e
challenge, 47f
license key, 47a
Unique e-content ID, 47b
value of transaction ticket, 47c
value of a relinquishing ticket, 47d
flag status 47e
challenge, 47f

FIG. 5A

FIG. 5B


unique terminal ID., 81a
private key, 81b
public key, 81c
device table of e-content licenses, 81d
key server
content server
License repository, 84
unique terminal ID., of terminal, that has license activated, 85a
License key, 85b
content ID. 85c
content ID, 83a
content file, 83

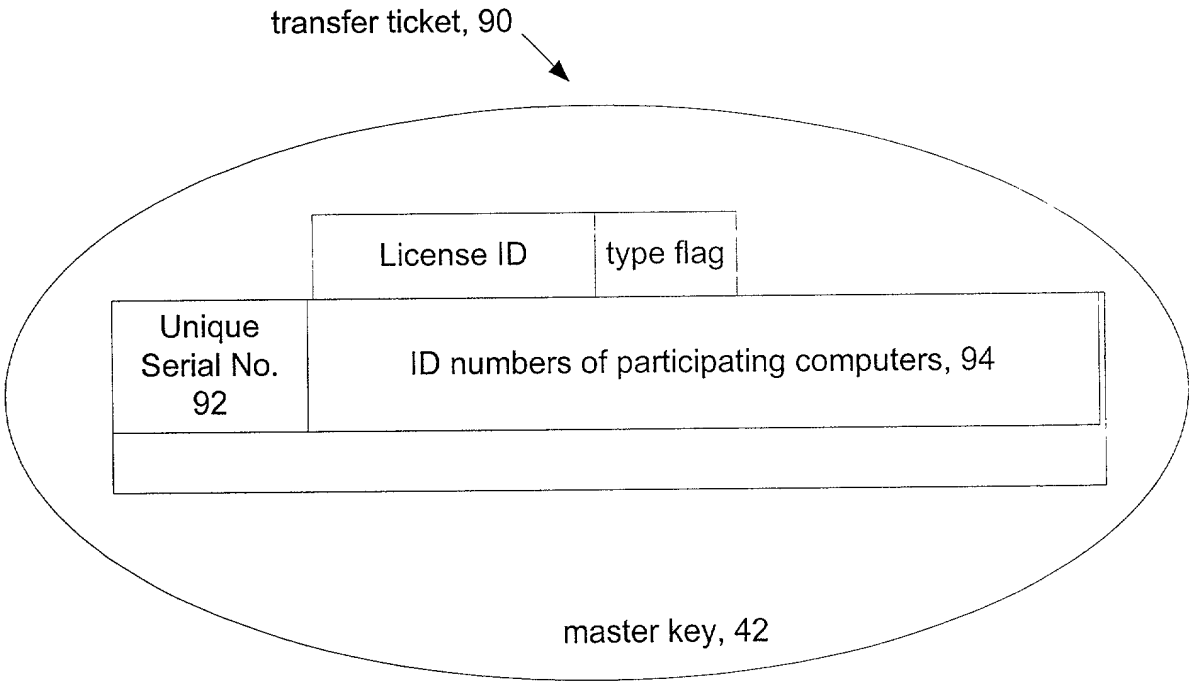


FIG. 6

Microsoft v. DataTern
Exhibit 1003
Page 0007

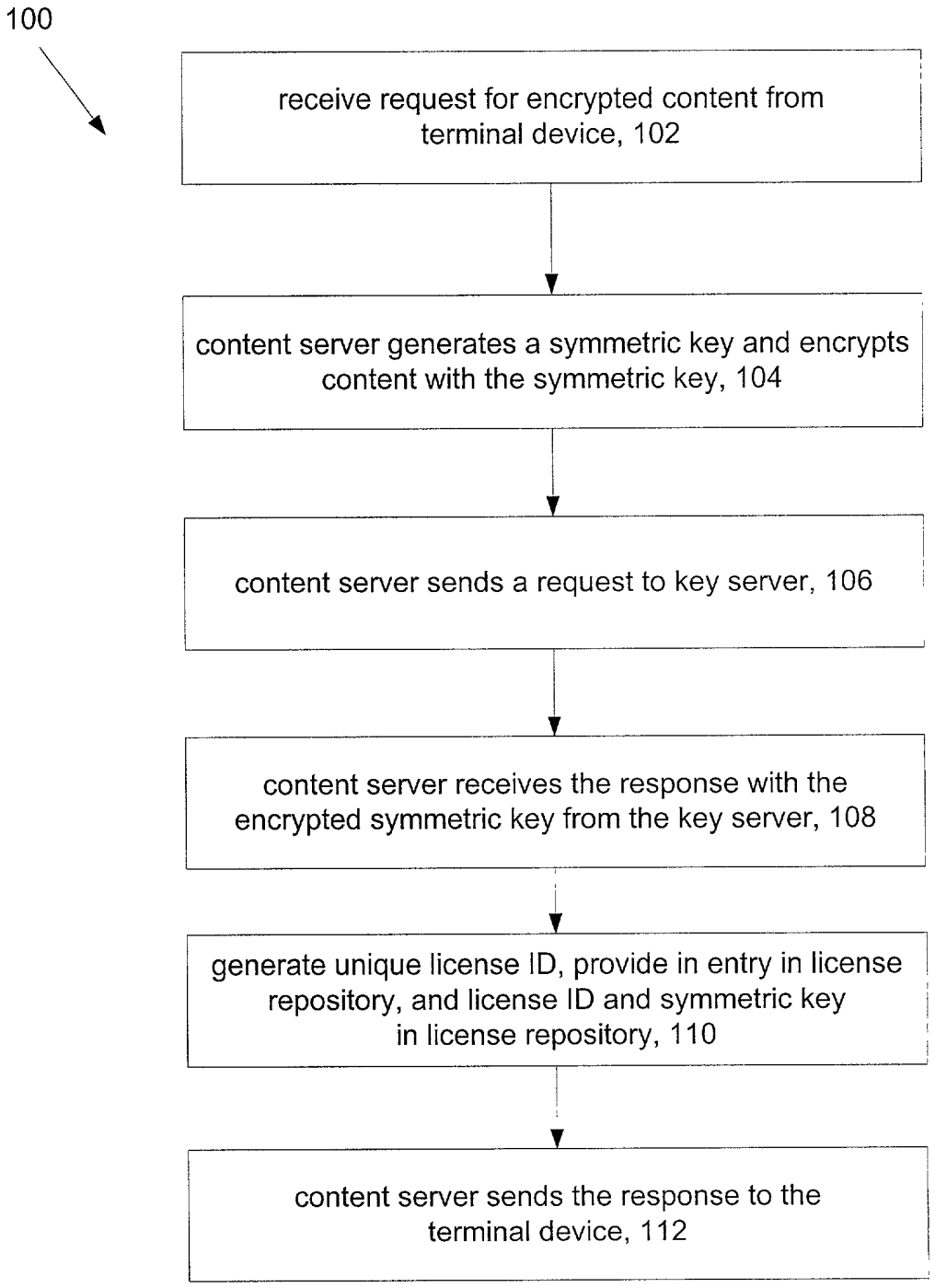

100
receive request for encrypted content from terminal device, 102
content server generates a symmetric key and encrypts content with the symmetric key, 104
content server sends a request to key server, 106
content server receives the response with the encrypted symmetric key from the key server, 108
generate unique license ID, provide in entry in license repository, and license ID and symmetric key in license repository, 110
content server sends the response to the terminal device, 112

FIG. 7

FIG. 8

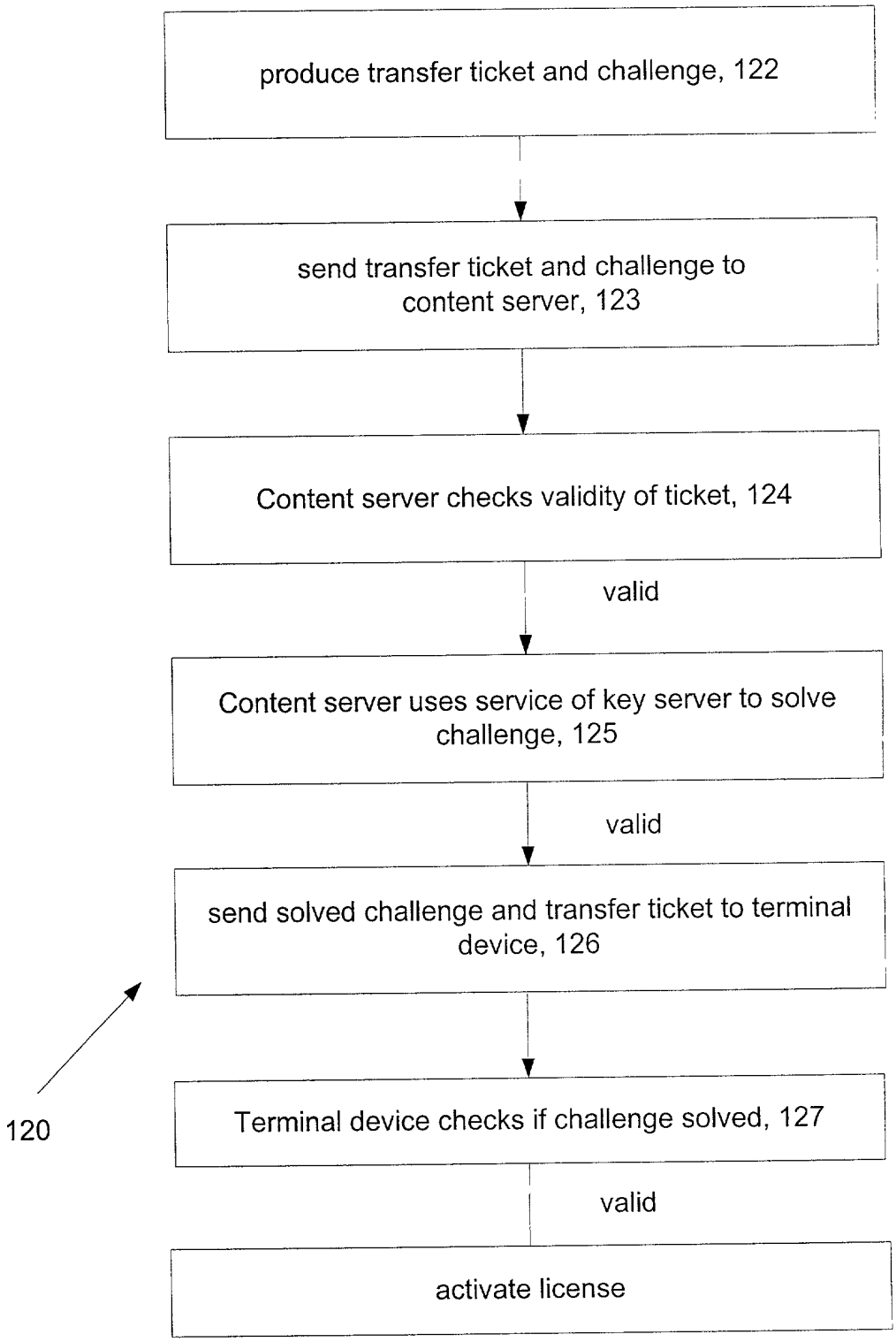
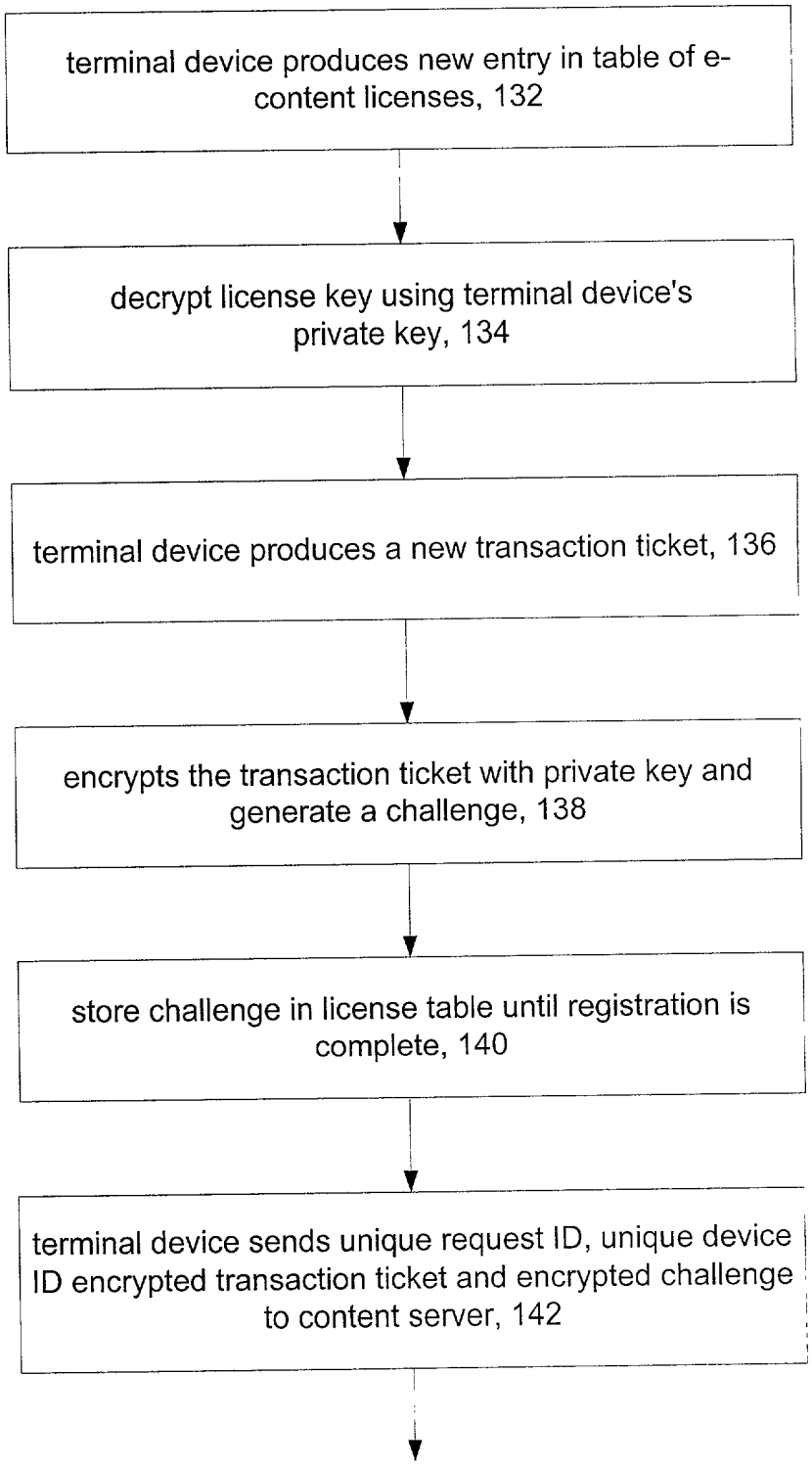

produce transfer ticket and challenge, 122
send transfer ticket and challenge to content server, 123
Content server checks validity of ticket, 124
valid
Content server uses service of key server to solve challenge, 125
valid
send solved challenge and transfer ticket to terminal device, 126
120
Terminal device checks if challenge solved, 127
valid
activate license

FIG. 9A


terminal device produces new entry in table of e-content licenses, 132
decrypt license key using terminal device's private key, 134
terminal device produces a new transaction ticket, 136
encrypts the transaction ticket with private key and generate a challenge, 138
store challenge in license table until registration is complete, 140
terminal device sends unique request ID, unique device ID encrypted transaction ticket and encrypted challenge to content server, 142

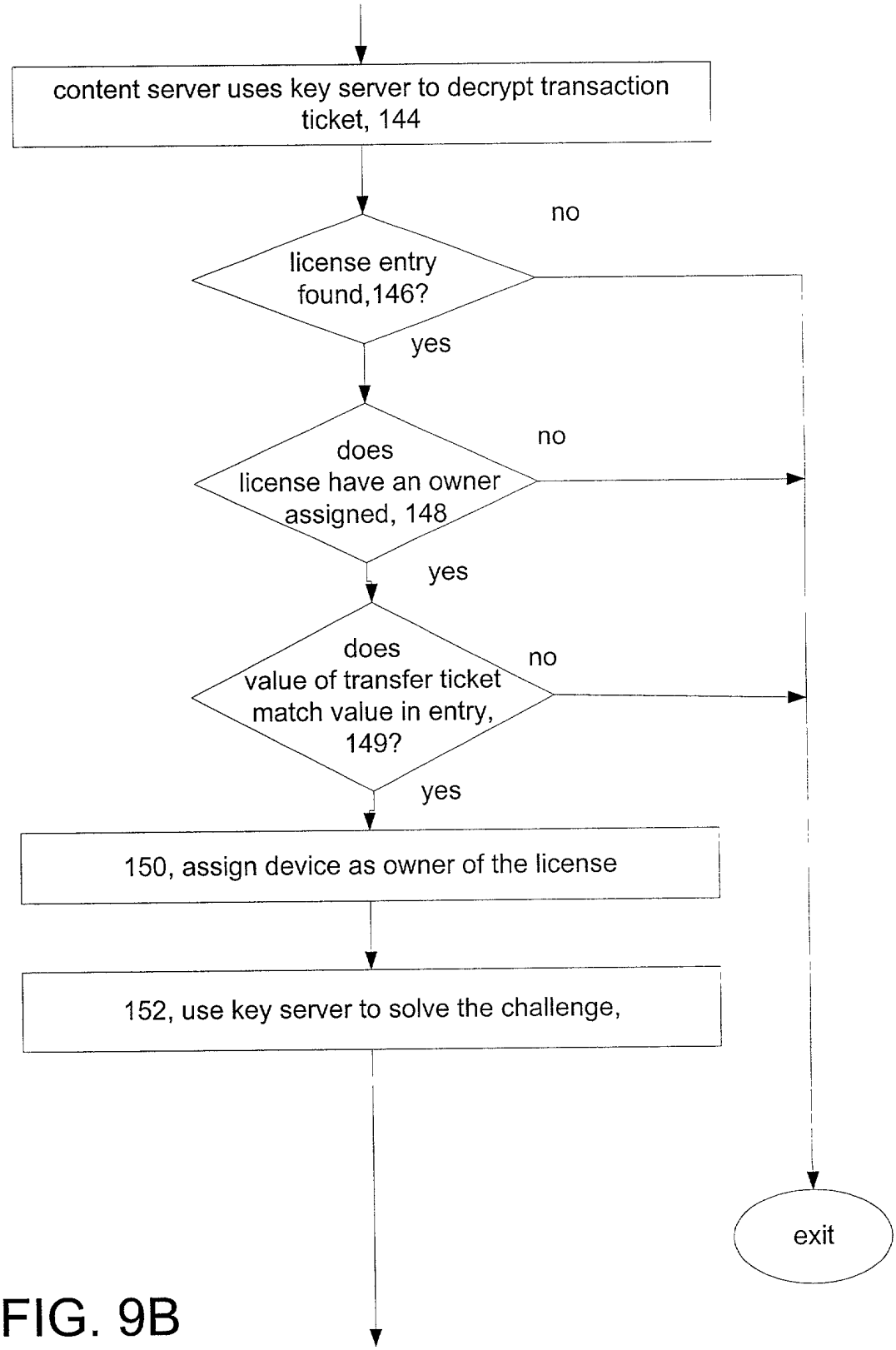

content server uses key server to decrypt transaction ticket, 144
license entry found,146?
no
yes
does license have an owner assigned, 148
no
yes
does value of transfer ticket match value in entry, 149?
no
yes
150, assign device as owner of the license
152, use key server to solve the challenge,
exit

FIG. 9B

Doc ID: US 2004/0054907 A1

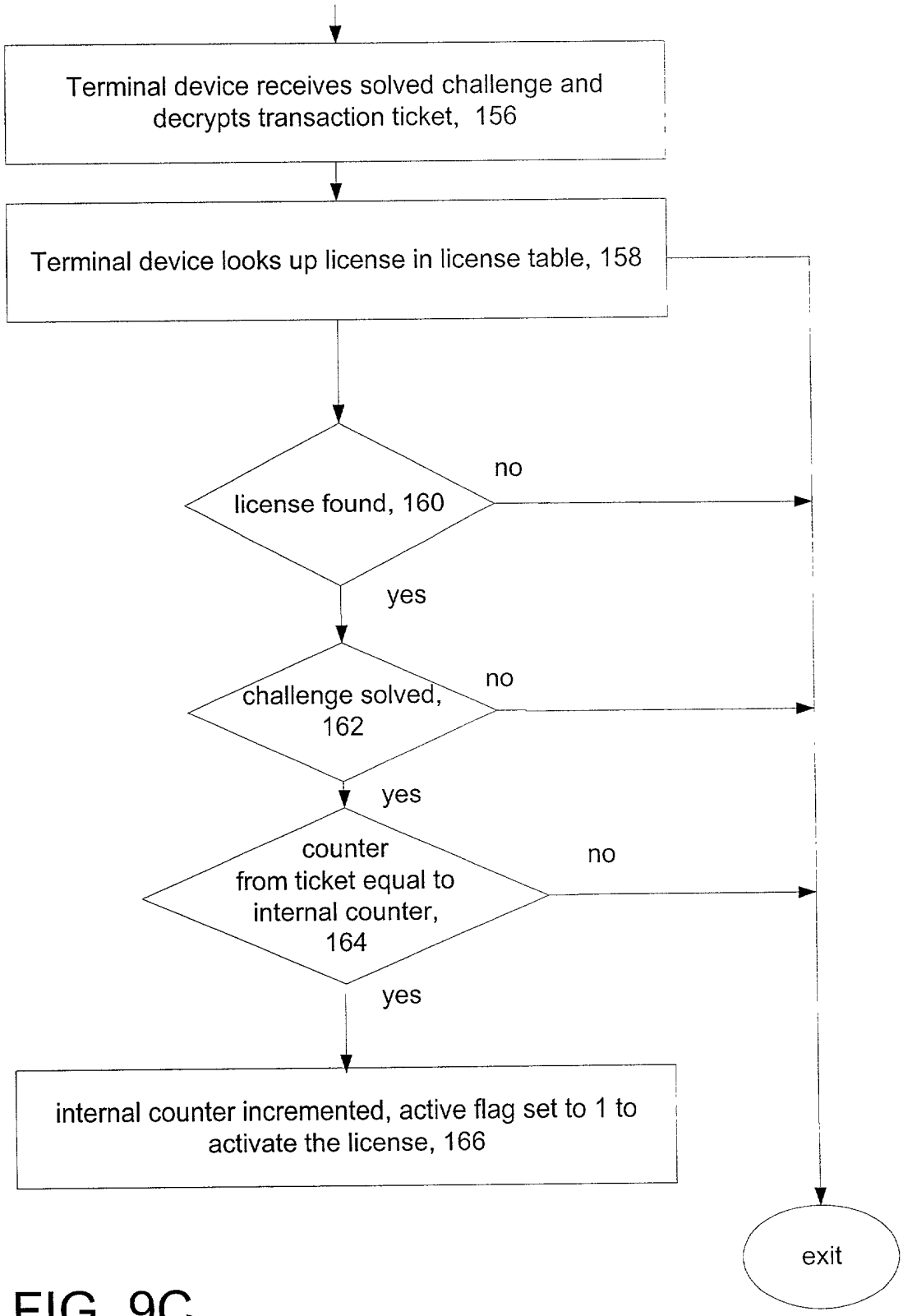


FIG. 9C

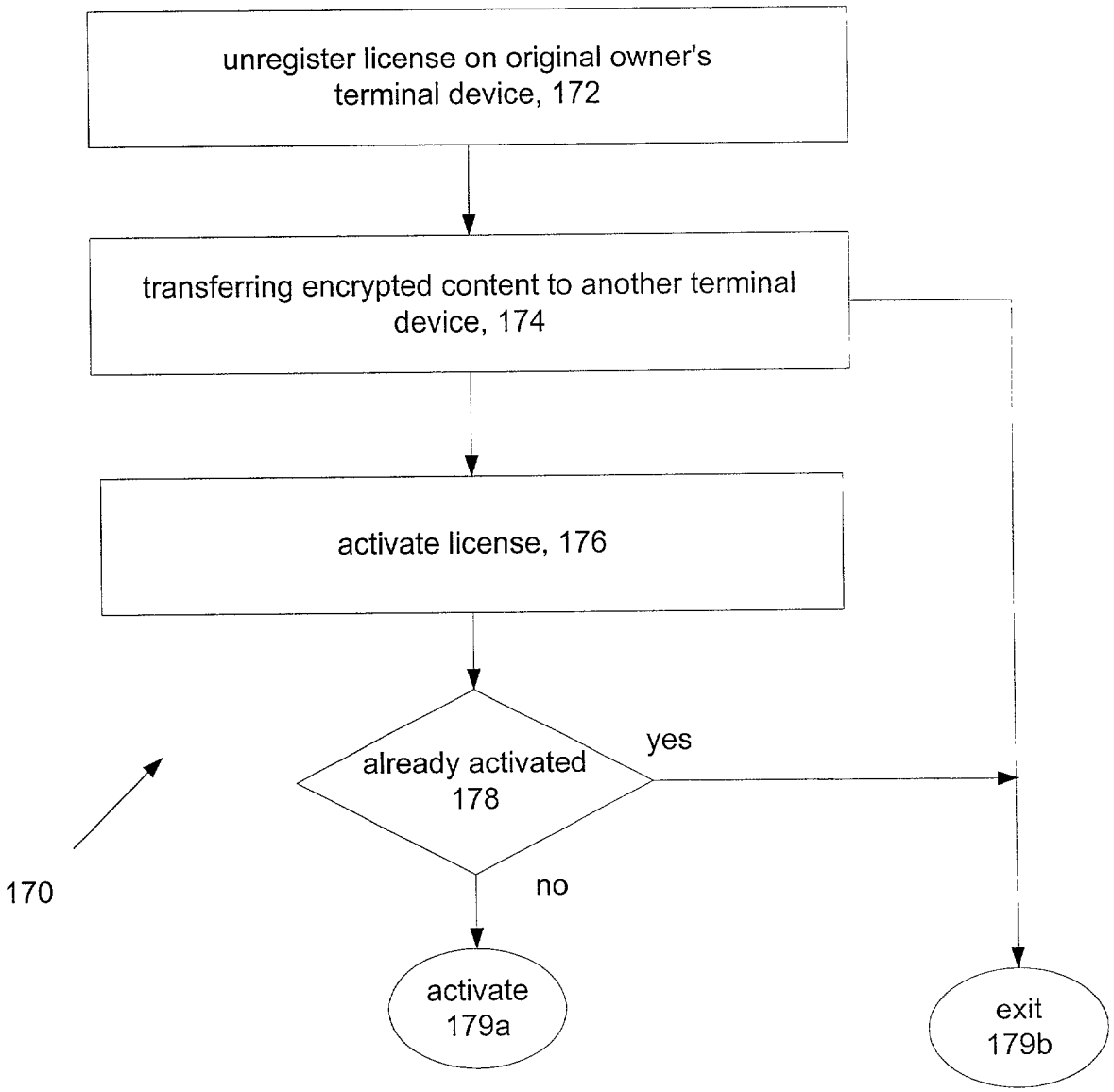

unregister license on original owner's terminal device, 172
transferring encrypted content to another terminal device, 174
activate license, 176
already activated 178
yes
no
170
activate 179a
exit 179b

FIG. 10

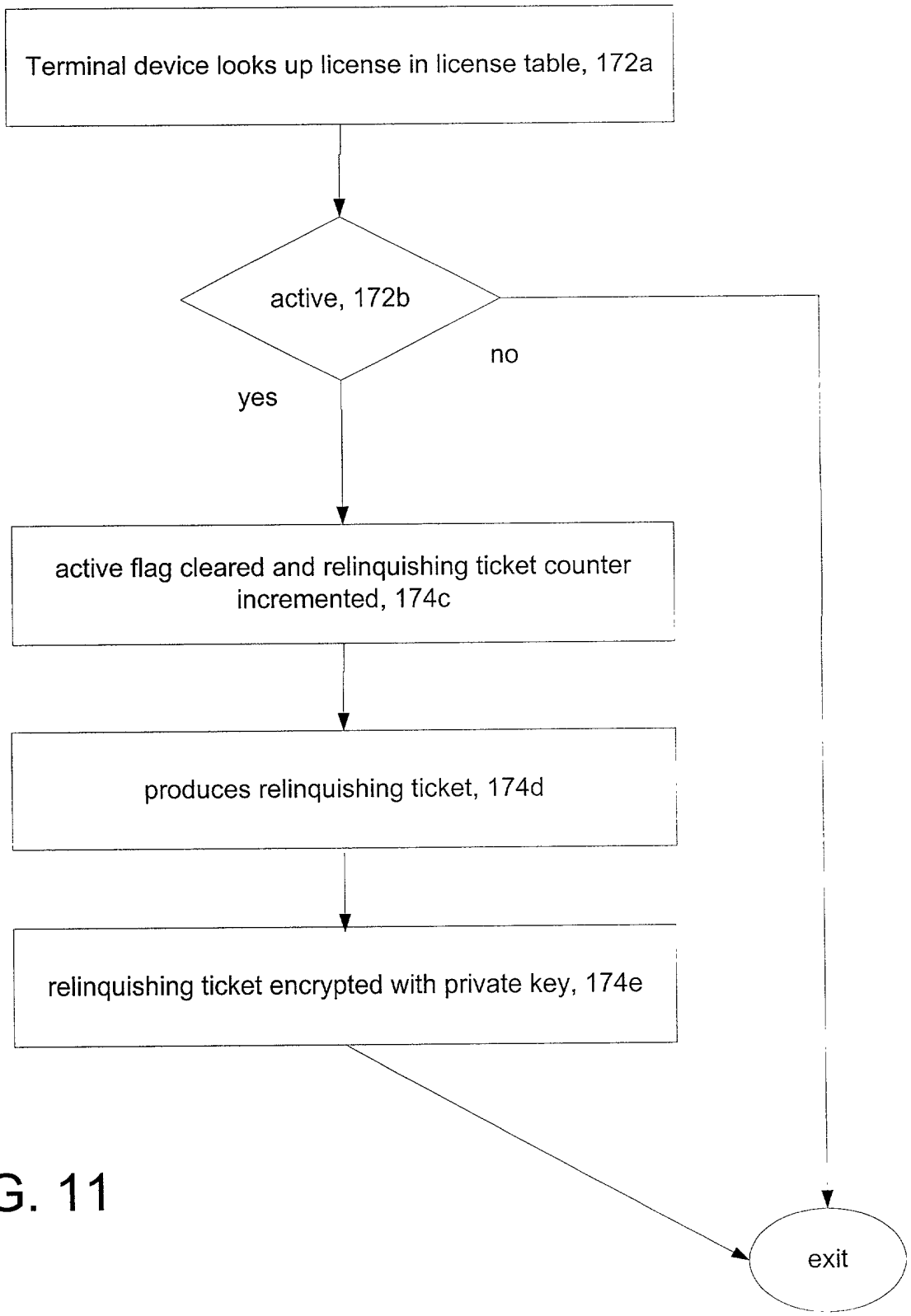

Terminal device looks up license in license table, 172a
active, 172b
no
yes
active flag cleared and relinquishing ticket counter incremented, 174c
produces relinquishing ticket, 174d
relinquishing ticket encrypted with private key, 174e
exit

FIG. 11

Docket No. 12782-002001

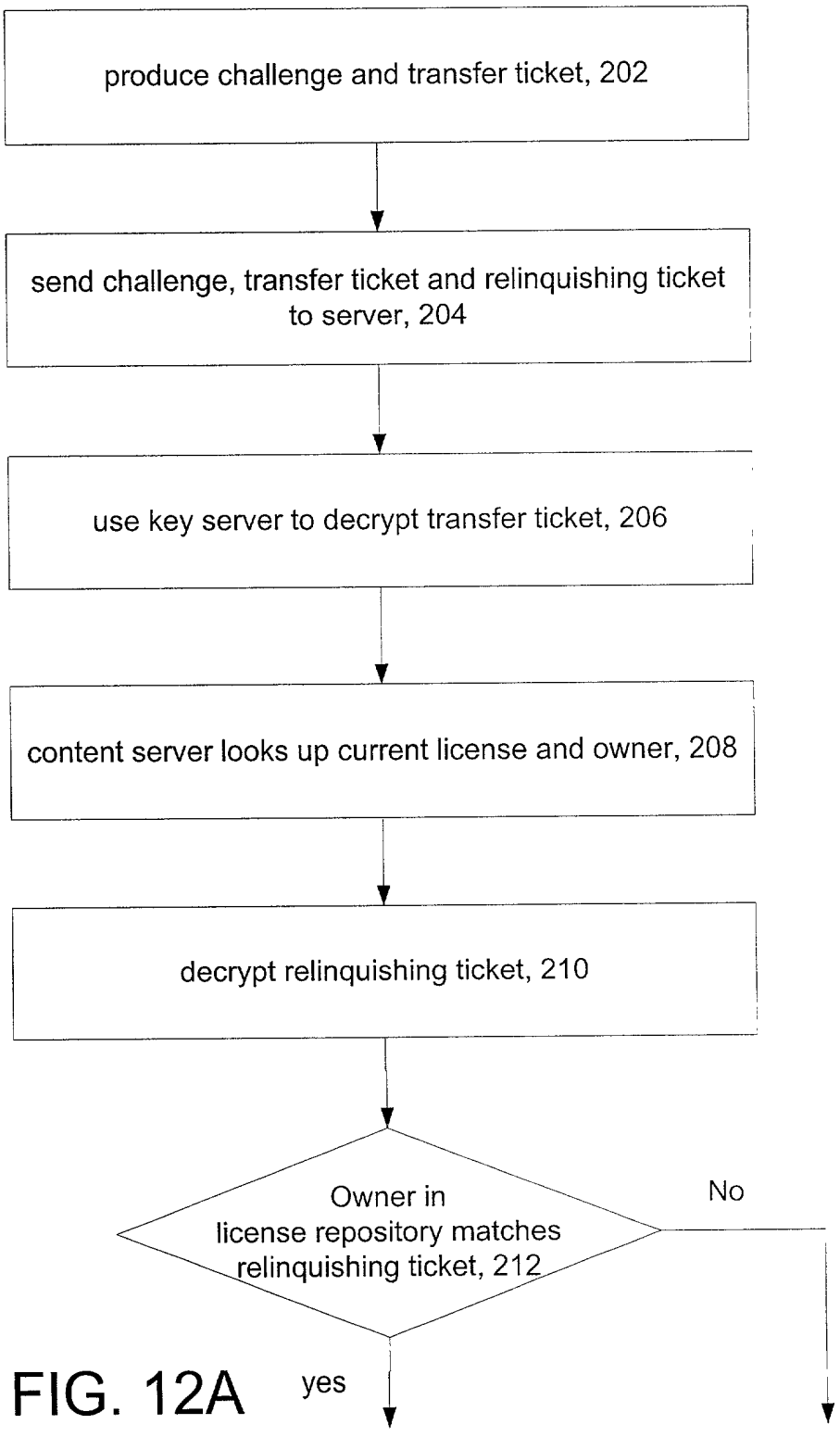


FIG. 12A

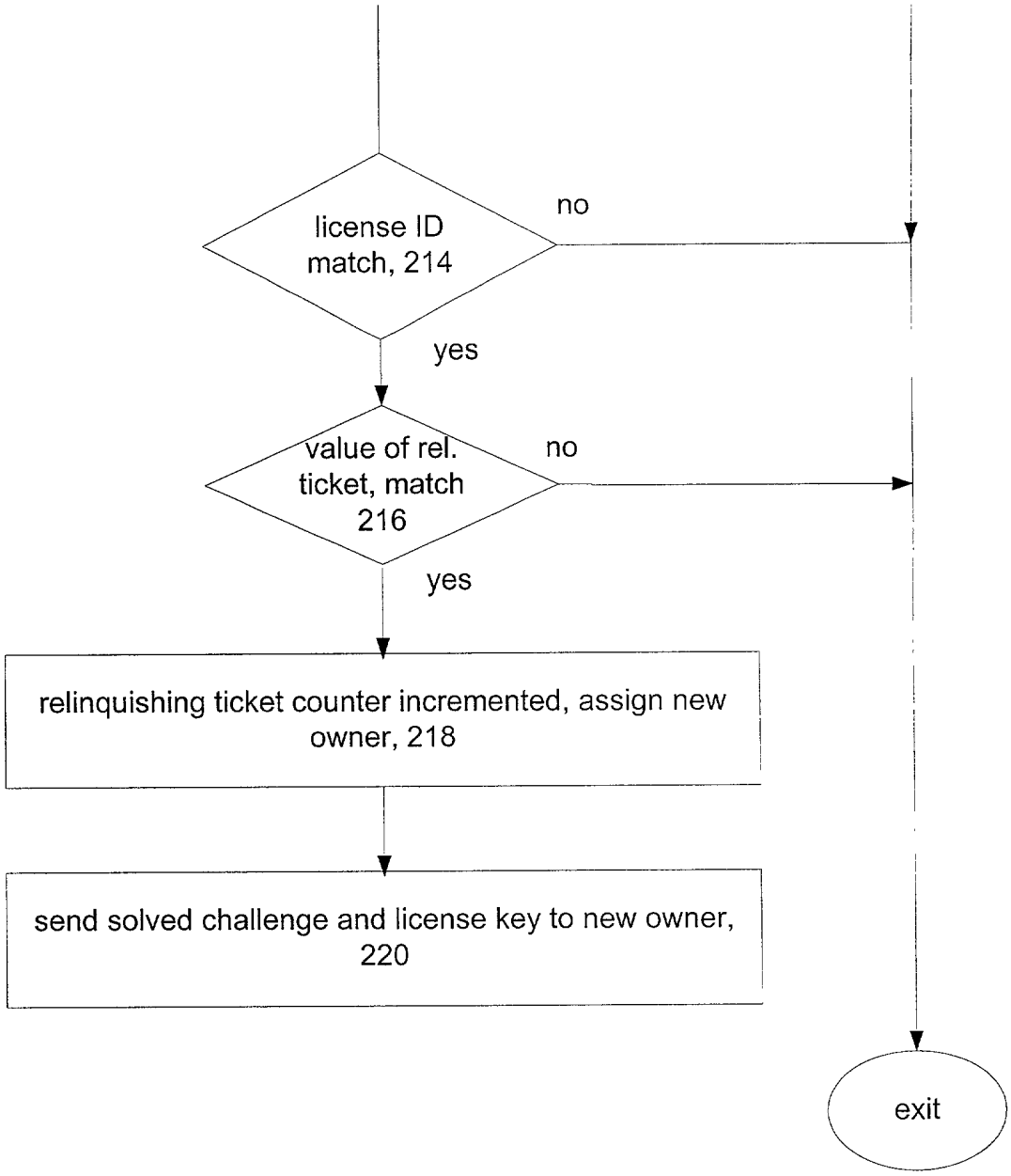

license ID match, 214
no
yes
value of rel. ticket, match 216
no
yes
relinquishing ticket counter incremented, assign new owner, 218
send solved challenge and license key to new owner, 220
exit

FIG. 12B

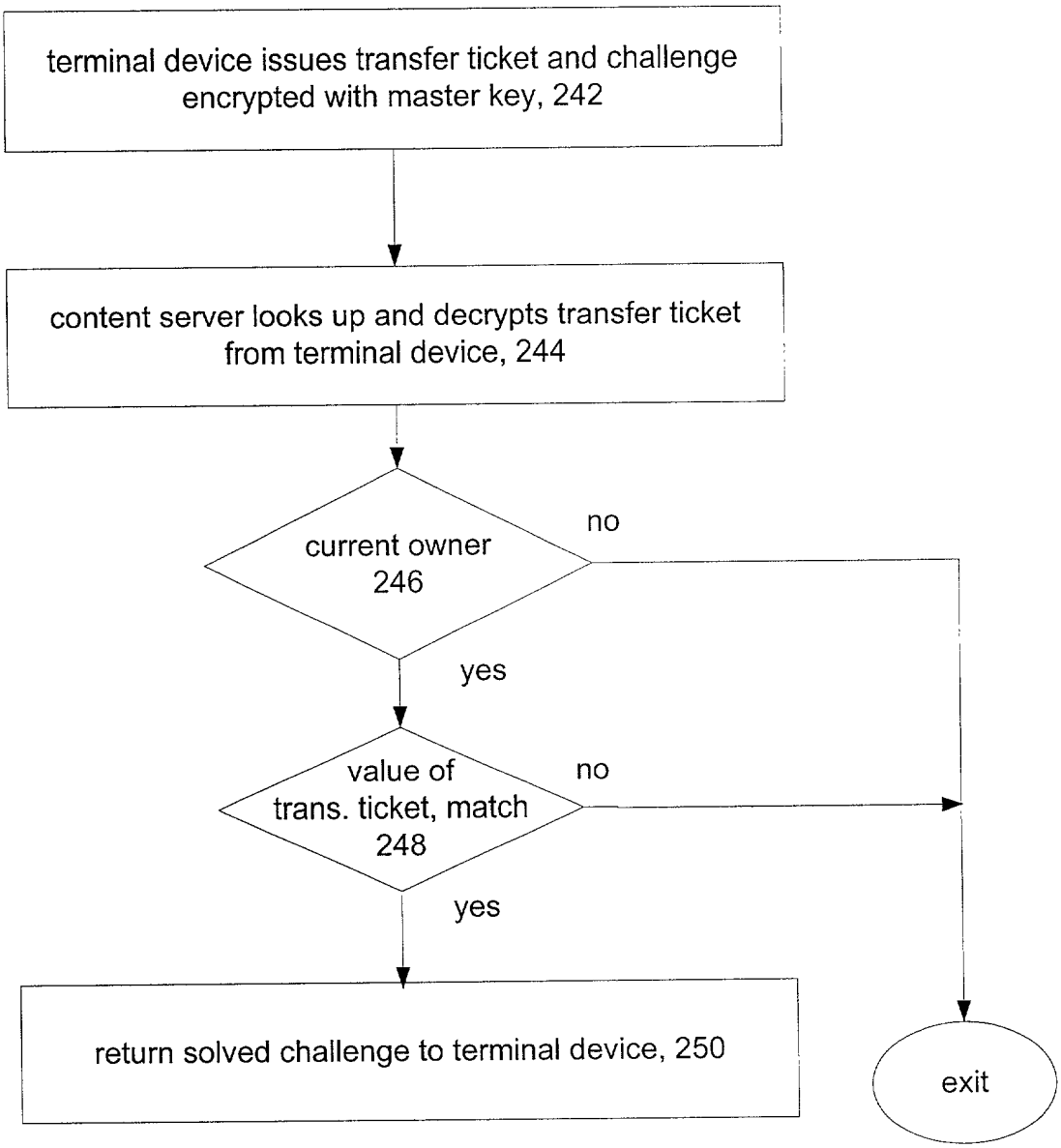

terminal device issues transfer ticket and challenge encrypted with master key, 242
content server looks up and decrypts transfer ticket from terminal device, 244
current owner 246
no
yes
value of trans. ticket, match 248
no
yes
return solved challenge to terminal device, 250
exit

FIG. 13